Successful Cyber Security in a Collaborative World

Jeff Mauth - PNNL
Scott Pinkerton – ANL
Brett Didier - PNNL

Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

Outline

- DOE Cyber Security Challenge
- Collaboration Benefits
- CPP-CFM Integration and Outcomes
- Going Forward
- Discussion

DOE Cyber Security Challenge

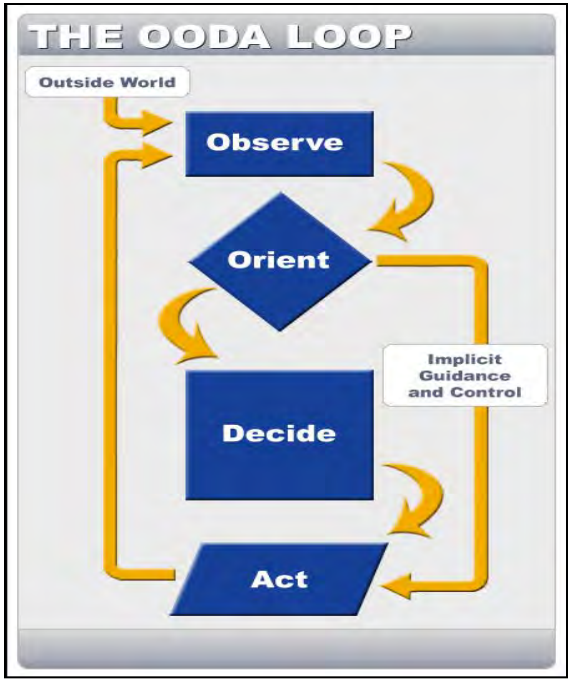
- ~70 unique entities operating ~130 facilities
- Mission driven work is highly collaborative and constantly evolving
- Cyber threats also evolving rapidly
  - Increasing skill & sophistication of bad guys
  - Std technology & common vulnerabilities
  - Increasing degree of connectivity
  - Increasing criticality of systems & data on-line today
- Threats are likely to be hostile at multiple DOE sites
- Rich in data but poor in information and communication

Current Practices are Primarily Site Centric

- Every site is a snow flake
  - Local approach to detection, analysis, and mitigation
  - Local approach to prevention (patching), user education, etc.
- Sharing typically through mandated reporting (not very timely)
- Difficult to quantify benefit of work/effort being leveraged rapidly and broadly
  - Collaboration is harder (especially in the security context)

Why Collaborate?

- Improve defense at local sites
- Improve our collective OODA Loop
  - Bad guys use collaboration as a tool – rapid dissemination/easy assimilation
    - Vulnerabilities publicized in chat rooms
    - Hacking tools bundled as software packages
- Coordinate as an army instead of operate as individual Cyber Samurais



Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

Collaboration as a Force Multiplier

"In cost benefit terms, technology-enabled collaboration acts as a "force multiplier." It reduces the time it takes for an individual to find the solution to a problem. The basic idea is that workers spend less time searching, and more time developing. In basic terms, "knowing the right people" in advance can reduce the time it takes to get questions answered, compared to getting that same question answered by having to start at "square one" without having access to such a network."

http://www.ddmcd.com/promoting.html

DOE Cyber Security Collaborations

- Network Security Monitoring Group
  - The people
- Cyber Fed Model Community
  - Near real time actionable information sharing
  - Scalable distributed message passing
- Cooperative Protection Program
  - Distributed Data Collection
  - Portal Community with Data Sharing Agreements
- DOE-CIRC
  - Tech Bulletins
  - Aware Portal
  - SiLC Server

Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

Building Successful Cyber Collaborations - aka Our Army

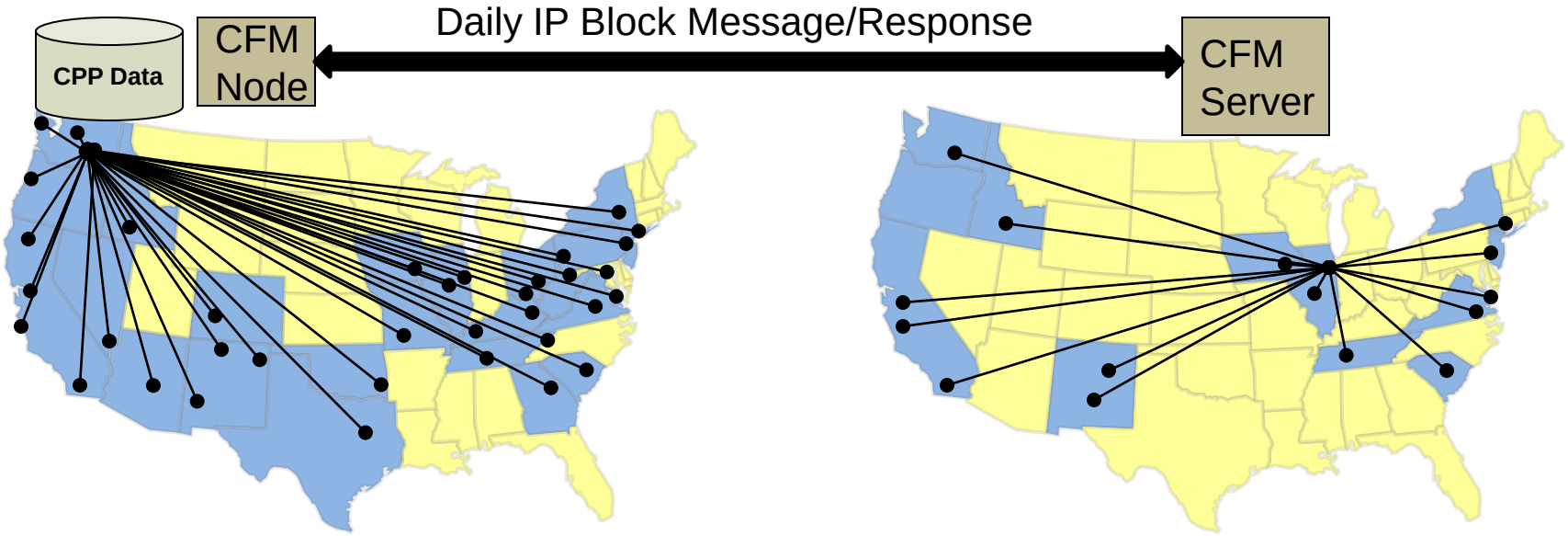
Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

What Did We Want to Accomplish with CPP/CFM Collaboration?

- Develop measures of efficacy for our cyber defenses
  - Timeliness of response
  - Threat overlap
- Prove value in collaboration for our cyber defenses
- Create a robust integration platform to build upon

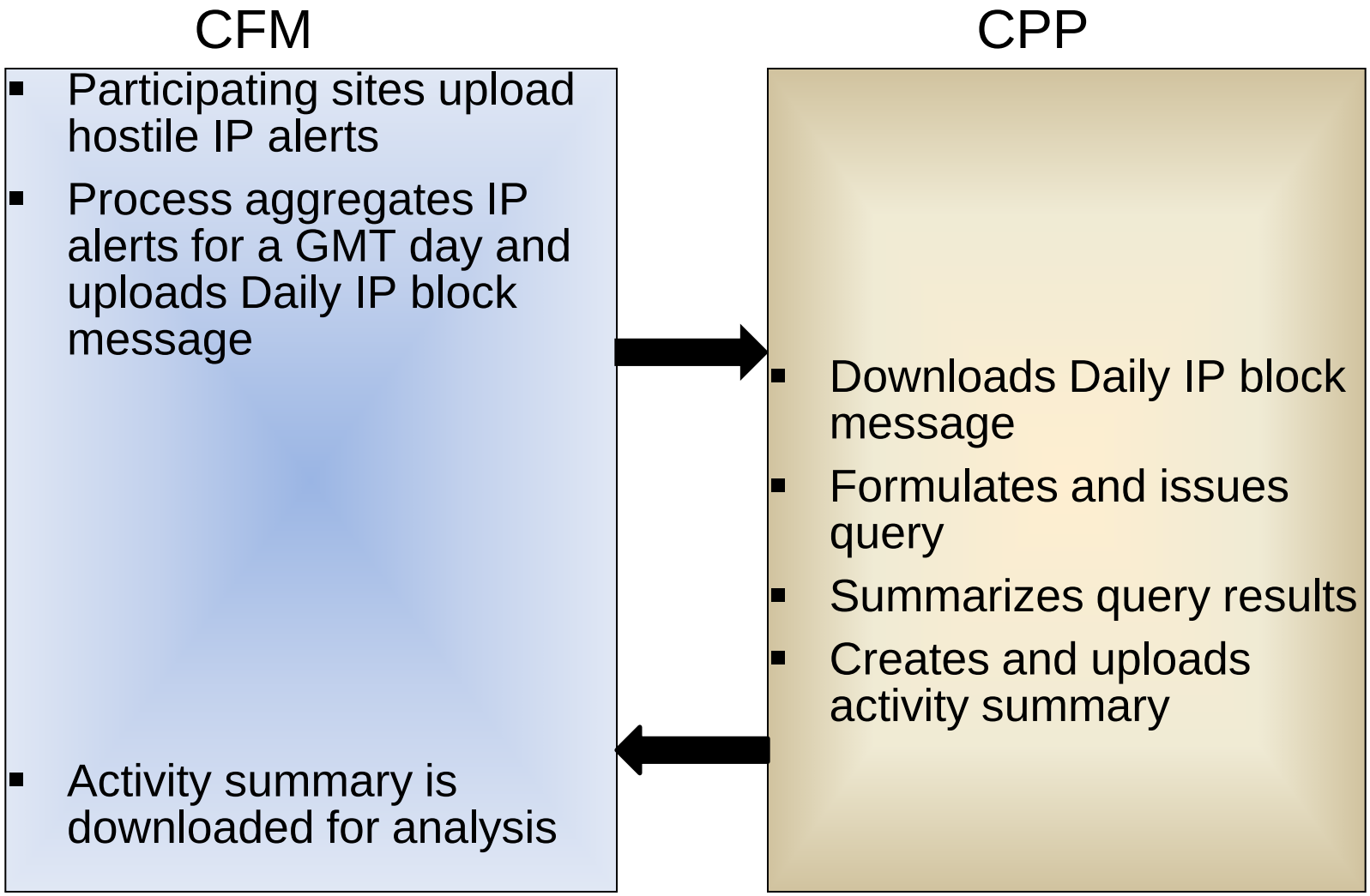
CPP/CFM Integration



Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

Current Integration – Daily Processing



Argonne NATIONAL LABORATORY

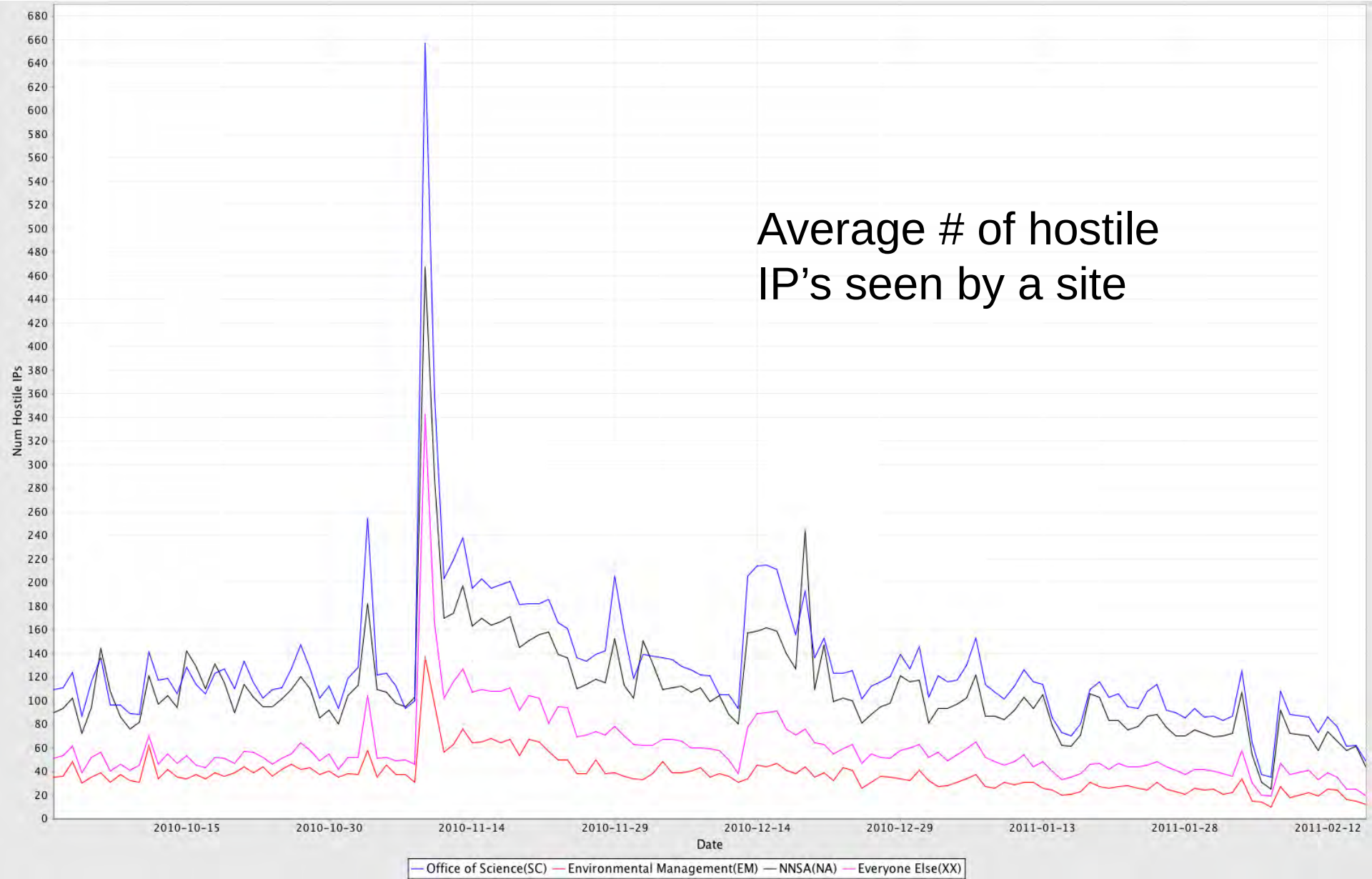
Pacific Northwest NATIONAL LABORATORY

Alerts From CFM – IP's Per Day

Relevance Across DOE Enterprise

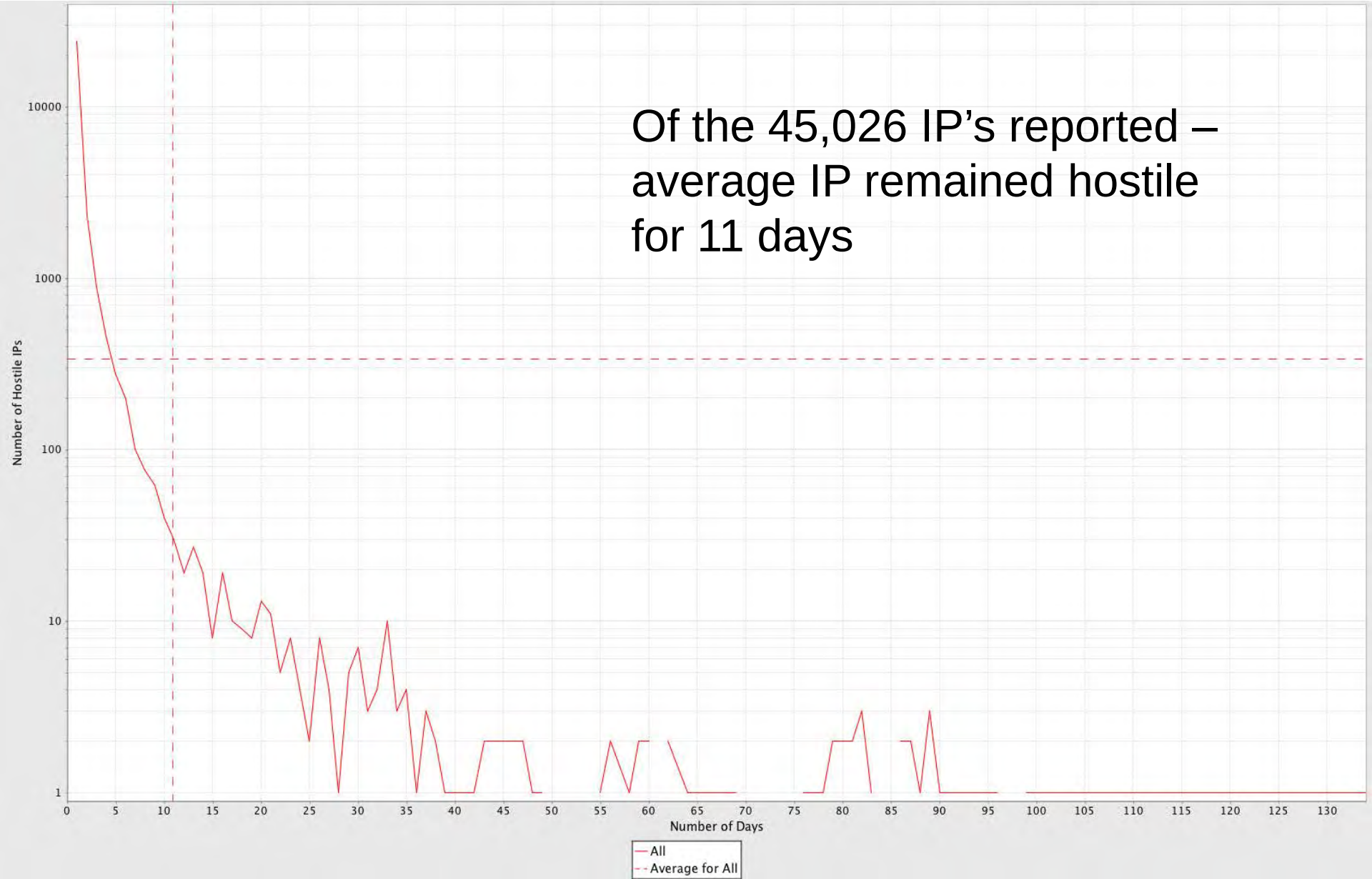
% of sites w/ traffic from at least one of the daily IP's

Collaboration Will Provide Local Benefit



Average # of hostile IP's seen by a site

Persistence of the Hostile IP's



Results of CPP/CFM Collaboration

- Significant overlap in sites with traffic from hostile IP's
- Timeliness of data is critical
  - Timeliness of decisions (OODA loop) is critical
- Incremental improvements in local detection capabilities can provide significant benefit to DOE's cyber defense
  - If we share best in class detection methods
  - If we share actionable information

Take Aways

- Sharing information is a force multiplier
  - Detect locally, React globally - act as an army
  - Heavy lifting is still required… timely sharing of in-depth analysis results will save significant effort across DOE

Argonne NATIONAL LABORATORY

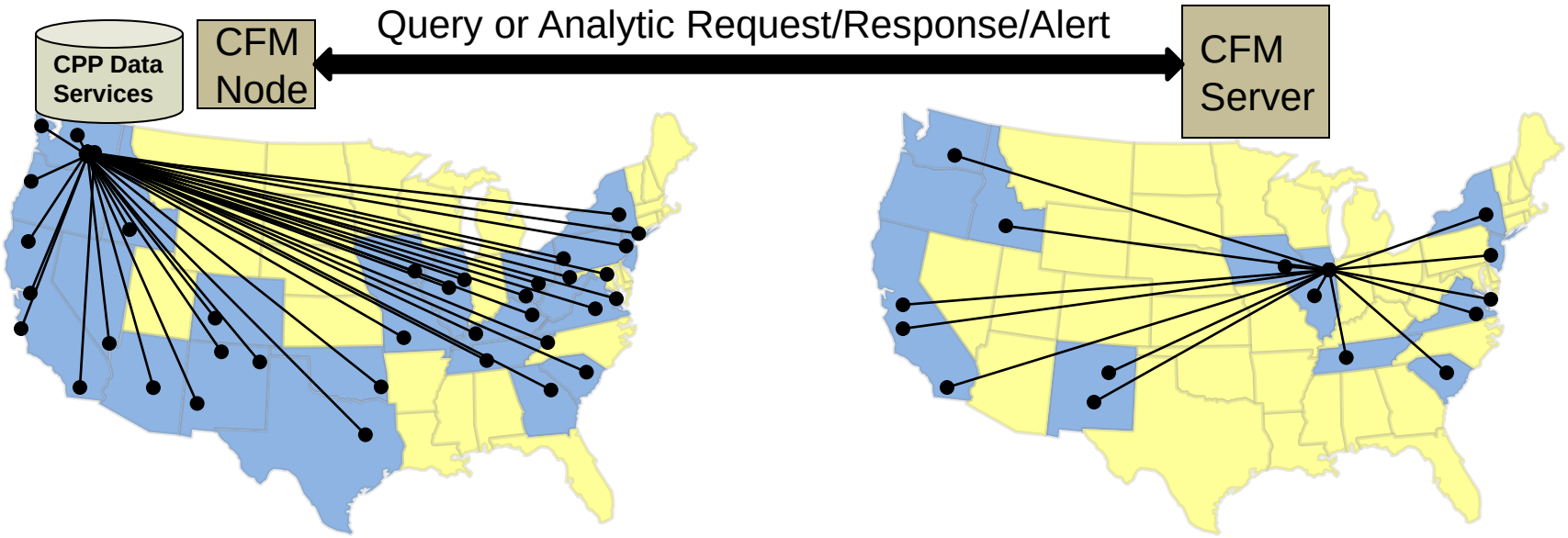
Pacific Northwest NATIONAL LABORATORY

Looking Forward

- We have integrated distributed enterprise data collection and distributed enterprise messaging services

- Many capabilities are now possible
  - Asynchronous queries/results of CPP data through CFM using CPP Sharing Policy
  - Analytical methods can be applied to CPP data and results distributed via CFM
    - Methods contributed by DOE Cyber Community
    - Hosted on CPP infrastructure
  - CFM alert notifications can be created based on analytical methods/algorithms running on CPP infrastructure

CPP/CFM Integration Path



Argonne NATIONAL LABORATORY

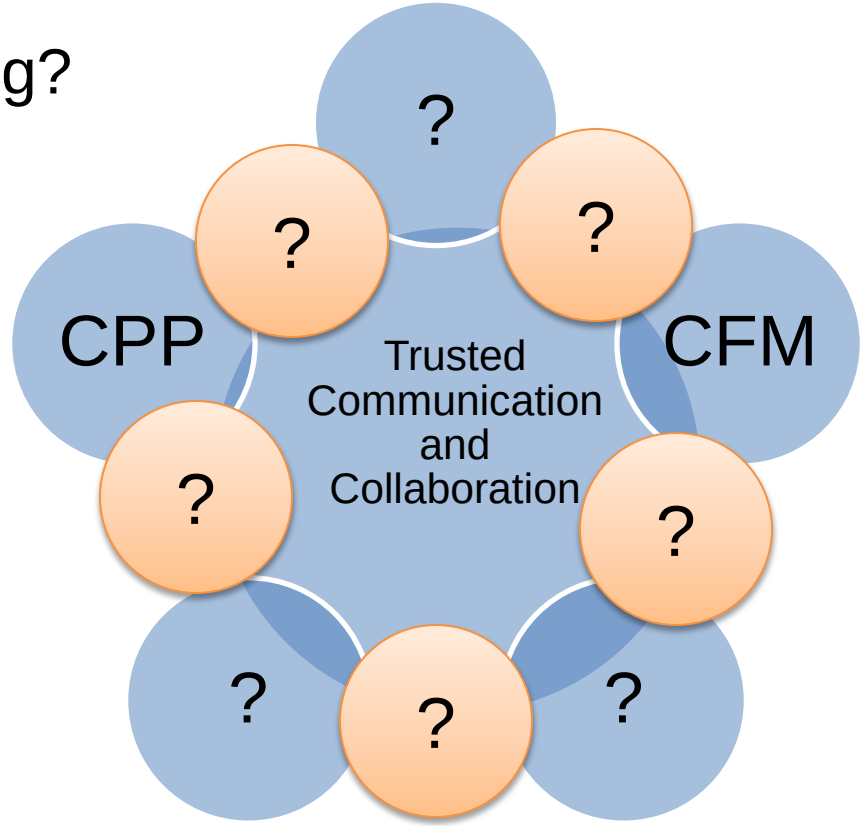
Pacific Northwest NATIONAL LABORATORY

How Do We Get There?

- Information sharing model
  - Treat access to CPP data through CFM the same as access through the Portal
    - Sharing controls enforced
    - Logging of queries
  - Analytical methods on CPP data that provide aggregate information is available for participating sites
    - e.g. I want to see ssh trending information for my site compared to all of DOE or all of Office of Science sites
- Accept community definition/contribution of analytical methods they want performed using CFM/CPP
- Increased community contribution of information

Where Do You Fit?

- Who should be participating?
- What can and should be shared globally?
  - Information
  - Tool assessment, configuration and methods
  - Mitigation/Recovery information
  - Resources (analysis/computing)
- What are your thoughts?

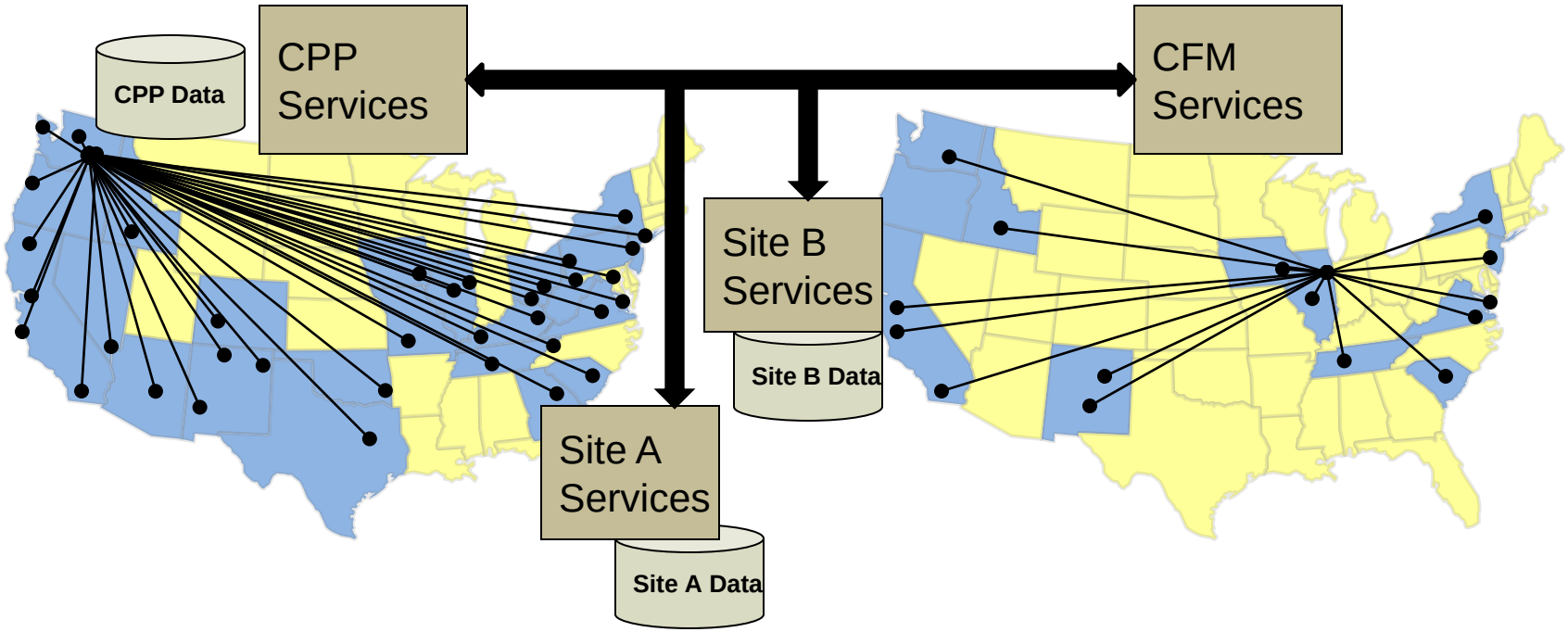


Comments/Discussion

Thank you…

- Jeff Mauth
- Scott Pinkerton
- Brett Didier

What Can You Contribute?



Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY